THE INDONESIAN JOURNAL OF BUSINESS ADMINISTRATION
VOL. 1, NO. 5, 2012: 301-311

IMPROVEMENT OF PT BANK XYZ AUTOMATIC TELLER MACHINE (ATM) QUALITY OF SERVICE THROUGH INFORMATION TECHNOLOGY RISK MANAGEMENT

Risky Nugraha and Sudarso Kaderi Wiryono
School of Business and Management
Institut Teknologi Bandung, Indonesia
fwm_risky@yahoo.com

Abstract—Technology has become one of the important factors in supporting an organization operational, especially in banking industry that relied heavily on information technology. Automatic Teller Machine (ATM) is one of bank e-channel products that provide the customers with the services that equal as doing transaction at the branch offices for 24x7 hours – spread throughout strategic location in all over Indonesia. With more than 6,000 ATMs that are spread throughout Indonesia, the banks can served billion rupiah of daily transactions that contributed as one of the banks source of revenue and also as one of its competitive advantage. In an attempt to increase its ATM quality of services as one of its competitive advantage, Bank XYZ periodically conduct internal audit on the ATM system to ensure the internal control is appropriate in protecting customer's data integrity and security while doing transaction. However, as time goes, the ATM system is also becoming more complex that cause the conventional audit method is not enough to detect flaws or weaknesses on the system that still exist and then improve it. It requires a new method to evaluate the system from banking services point-of-view. Risk-based audit method that is focused in ATM services, enable Bank XYZ to identify risks for each possible scenario when customer doing a transaction at ATM. By using that method, it is expected to improve Bank XYZ ATM quality of services to fulfill its ATM level of service claim – 24x7 hours of banking services through risk mapping prioritization method.

Keywords: ATM, Information System, IT Audit, IT Risk Management

I. INTRODUCTION

Technology has become one of the important aspects in human life, which also occurred in the banking world where technology is becomes something crucial. The application of advanced technology has become one of the benchmark points from the bank's customer point-of-view to evaluate the bank performance in providing their services. *Automatic Teller Machine* (ATM) is one of electronic banking products that become the backbone in the continuity of the bank services which provided bank's customers with flexibility and convenience to use. Using ATM, bank's customers are enabled to do transaction for 24 hours, seven days a week, without the need to call the bank's branch offices. Through continuous improvement in quality and quantity of ATM, banks hope to meet customer satisfaction which is one of the important aspects to achieve its goals. Bank XYZ as one of the largest bank in total assets in Indonesia is also aware about those facts and periodically invites external or 3rd party organization to do an analysis about the current ATM system to find any opportunity to improve further the system and author has been invited as a team to find any weakness points or potential problem on the ATM system.

PT Bank XYZ Tbk. (Bank XYZ) was formed on October 2, 1998 as part of the Government of Indonesia's bank restructuring program. In July 1999, four state-owned banks amalgamated to become Bank XYZ. Each of the four legacy banks played an integral and essential role in the development of the Indonesian economy. Bank XYZ is now embarked on the second stage of its transformation process for the 2010-2014 periods, during which time the Bank has revitalized its vision "To be Indonesia's most admired and progressive financial institution".

During those periods, bank XYZ business activities are focus on the following three business areas:

1. Wholesale Transaction
2. Retail Deposit & Payment
3. Retail Financing
4. Cash Management
5. Treasury Services
6. Insurance
7. Government Bond and Mutual Fund (Reksadana)
8. Retail Brokerage

This research was conducted in bank XYZ Directorate of Technology and Operations which is responsible in managing all the information systems run inside Bank XYZ. Directorate of Technology and Operations has served an important role through boosting its operational efficiency, implementing

technology solutions, increasing operational capacity and amplifying its economies of scale by consolidating operational units.

II. BUSINESS ISSUES EXPLORATION

As explained in the previous section, Directorate of Technology and Operations has important responsibility in developing and maintenance the ATM system & service through its groups consists of IT Planning, Architecture & BCP group, IT Strategic Business Solution, IT Application Services Group and IT Operations Group. However, those groups used to be driven by ATM technology vendors which only care about per unit system performance and never looked from the whole ATM services. That is a serious problem for a financial institution with the responsibility to provide excellence services to its customer. That problem is also causing the groups under this directorate fully depend on what vendors said and barely have any method for the internal to improve the ATM system.

The impact of those problems from the customer point-of-view, the continuous ATM system improvement is obstructed and the current ATM system is no longer can support the bank XYZ ATM service tag line "24x7 hours of banking services" as the fact on the current ATM system cannot fulfilled it and for the internal bank XYZ, this current system may responsible in increasing in its operational cost every year which may impact the financial performances on the future.

A. Conceptual Framework

As defined above there are currently two major issues on bank XYZ ATM services, obstructed ATM system improvement and vendor driven on the ATM system. However, it is too early to define the root without deep analysis to the bank XYZ groups or units who's responsible with the ATM and also the how the ATM system works itself.

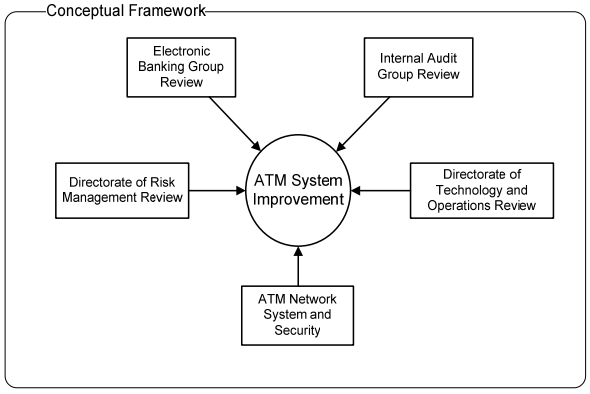

Figure 1. Conceptual Framework

The conceptual framework of this research is generated to explore the business issues on bank XYZ ATM service related with its current ATM network system. With a clear exploration on the business issues, this research could determine the root of the problems and enable to provide bank XYZ with necessary business solution furthermore.

B. Issues Data Collection

According to the conceptual framework defined before, the business issues exploration would be carried out by reviewing Bank XYZ Electronic Banking Group, Internal Audit Group, Directorate of Risk Management, Directorate of Technology and Operations to know it roles and discovered any existing method to improve the ATM system. It also necessary to know and understand the process in bank XYZ ATM Network System and Security to identify any potential problems that may occurs. In collecting the data for the business issue analysis, researcher did interview with the responsible staff and also read the documents related to the ATM system about the responsible for each directorate or groups and also the ATM network system topology.

The results of this method are several findings on the following list for each points on the conceptual framework that has influence on the ATM system improvement:

1) **Electronic Banking Group** is responsible in designing and managing ATM services or features and in expanding the ATM network system all over strategic location in Indonesia.
2) **Internal Audit Group** is responsible in auditing the people, process, and procedure during ATM system project development phase, implementation phase and operational phase.
3) **Directorate of Risk Management** trough its Corporate Risk Group is responsible in providing risk management framework and tools for units or groups responsible in developing ATM system and services before, during and after the ATM project development phase.
4) **Directorate of Technology and Operations** is responsible in developing and maintenance the ATM system & service through its groups consists of IT Planning, Architecture & BCP group, IT Strategic Business Solution, IT Application Services Group and IT Operations Group.
5) **Current ATM Network System and Security** has five main problems that being neglected by bank XYZ which are:
   - **Problem-1**
     Daily critical down time – Full System Offline for maximum 12 minutes
   - **Problem-2**
     Tandem partition storage monitoring procedure
   - **Problem-3**
     Tandem password security vulnerability
   - **Problem-4**
     Base24 password security vulnerability
   - **Problem-5**
     ATM technology specification and implementation used to be driven by vendors

From those five problems above, there are five possible scenarios that may trigger risk events.

- **Scenario-1**
  Derived from problem: 1, 5
  "*Customer is doing a payment or transfer or withdrawal transaction, while waiting the transaction to be executed completely, daily critical down time executed by the operator which caused the transaction failed to execute properly while it is already charge to the customer balance*".
- **Scenario-2**
  Derived from problem: 1, 5
  "Daily critical down time exceeding the maximum time limit that caused customers who want to do a transaction during those down time have to wait longer than they expected".
- **Scenario-3**
  Derived from problem: 1, 5
  "During daily critical down time, ATM has been tampered and reset by irresponsible party that is difficult to detect by Bank XYZ's operator".
- **Scenario-4**
  Derived from problem: 1, 2, 5
  "Operator either intentional or unintentional did not execute tandem machine storage maintenance at the end of month or 35 days so the tandem storage level reached the 10% empty space storage limit and let the tandem system down which severed all the ATM system".
- **Scenario-5**
  Derived from problem: 1, 3, 4, 5
  "During daily critical down time, operator are using the password to login to tandem machine for monitoring from several terminals and then an irresponsible staff either intentional or unintentional conduct customer data transaction manipulation on tandem database".

C. *Analysis of Business Situation*

From the several findings explained before, it can be concluded that bank XYZ Electronic Banking Group together with Corporate Risk group and IT Operations Group are responsible in continuously improving its ATM system. This conclusion derived from the facts that Electronic Banking Group is responsible to gather customer feedback about the ATM services, Corporate Risk Group is responsible for identify any inherent risk from the current ATM system especially any risk event that can influence customer inconvenience in using ATM, and IT Operations Group that responsible in maintaining and troubleshooting on the ATM system.

However, bank XYZ barely have any method or procedure to improve the current ATM system, even though Corporate Risk Group said it has *Enterprise Risk Assessment Voting System* as a tool to help in improving bank XYZ service performances through manage the risks found by each individual or business unit, but it is barely known among bank XYZ employees and it existences is also cannot be confirmed. Based on those facts, it can be concluded that the root problem of the business issues is there is no practical method or procedure in bank XYZ that can be used by any individual or business units to help in improving the current or implemented ATM system. This root cause also the reason why bank XYZ is mostly fully depend on the 3rd party vendors to improve the system without doing any internal analysis first.

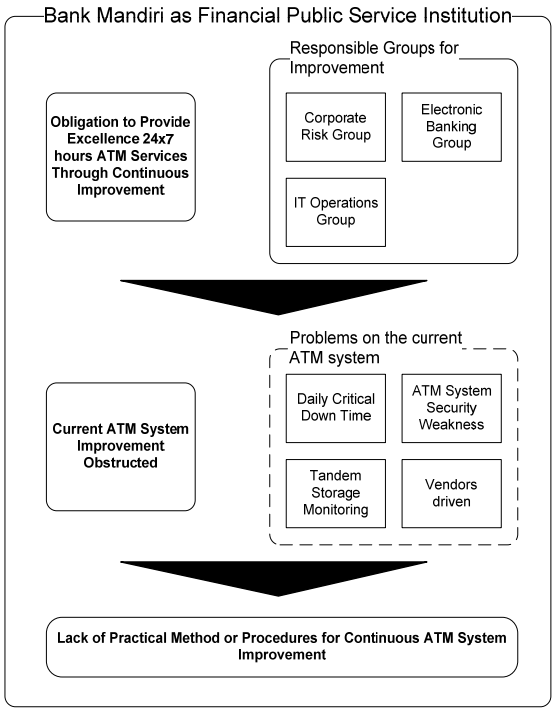

Figure 2. Root Cause Diagram

III. BUSINESS SOLUTION METHODOLOGY

In developing appropriate methods or procedures, researcher was considering using between the Conventional IT audit methods or Risk-based IT audit method. In practical, those two methods are not replacing each other. Instead, they are complementing each other and each of them has its different roles that will explain below.

A. *Alternatives of Business Solution*

The following tables are the comparison between Conventional IT audit method vs. Risk-based IT audit method according to Audittindo Education (2006).

TABLE I. IT Audit Method Comparison

Characteristic	IT Audit Method	
	Conventional	**Risk-based**
Audit focus of attention	Internal Control	Risks that can affect business operation
Audit response	Reactive: act as an observer in strategic planning	Co-active: involved in strategic planning
Risk evaluation method	Analyze risk factors from the internal control	Analyze the risk from the scenario created from scenario planning
Audit target	Important internal controls	Important risks
Audit recommendation	Internal Control: • Strengthen • cost-effective • effective/ efficient	Risk mitigation: • Avoid • Transfer • Control • Retain

As can be seen on the above table, Risk-based IT audit method is more appropriate to use as tool in improving the ATM system as this method evaluate the information system from whole system flow interconnect with all business aspects in an organization.

B. Business Solution Implementation

There are many standards in risk management that can use as references in designing risk management framework in an organization. One of the standards that widely used in risk management designed by the *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) that provide consistent guideline in risk management practices and also provide model that can accept throughout across organization. Based on COSO framework, in this project researcher proposed a risk-based IT audit framework that can be used by any individual or business unit in bank XYZ to improve the ATM system. The propose framework consists of stages explained below:

- *Stage-1:* ***Set the Context***

Project Description

Organization : PT Bank XYZ Tbk.
Location : Bank XYZ Head Office
Risk Owner : Bank XYZ Operational
Risk Scope : ATM system and its security
Project Goals : ATM system improvement related to ATM quality of services
Project Objectives :
- Identify current ATM system weaknesses
- Identify the risk
- Assess the risk
- Prioritize and mitigate the risk
- Build risk report

Risk Appetite : Most employees have an intuitive understanding of what level of risk they can take and the organization itself is quite open in considering all potential option in order to reduce the overall risks which can be seen from organization policy to give reward for good contribution in risk management.

- *Stage-2:* ***Risk Identification***

The risks identified from the five problems defined before are listed on the following table with its scenarios defined before.

TABLE II. Risk Event and Potential Loss

No.	Event description & Scenarios	Type of risk	Category of risk	Potential loss
1	Poor acceptance of ATM services by customer ***Scenarios: 1***	Business	**Strategic**	Low ATM transaction frequency lead to decline in revenue
2	Competitor offer better ATM system for customer ***Scenarios: 1***	Business		Low ATM transaction frequency lead to decline in revenue
3	Losing customers due to unsatisfied with the ATM services ***Scenarios: 1, 2, 4***	Business		Decline in revenue
4	Customer failed to pay his/her debt obligation ***Scenarios: 1, 2, 4***	Credit	**Credit**	Decline in earnings and NPL arise
5	Data center security violation ***Scenario: 5***	People	**Operational**	Customer trust & write down
6	Fraud on payment server ***Scenario: 3***	People		Customer trust & restitution
7	Change of requirement on the current system ***Scenario: 1, 2***	Process		Loss of recourse
8	Limit budget on system maintenance ***Scenario: 4***	Process		Loss of recourse
9	Data center not enough storage ***Scenario: 4***	Process		Write down
10	Fail to follow-up and solve problems from customer complain ***Scenario: 1, 2, 4***	Process		Customer trust and restitution
11	Data center overload due to poor load balance estimation	Productivity		Loss of or damage to asset

	Scenario: 4			
12	Particular network system failure due to human error ***Scenario: 2, 5***	Productivity		Loss of or damage to asset
13	Particular network system failure due to defect network hardware ***Scenario: 2***	Technology		Loss or damage to asset
14	Particular network system failure due to software bug or virus ***Scenario: 2, 3, 5***	Technology		Loss or damage to asset
15	Fraud on ATM payment mechanism during regular downtime ***Scenario: 3***	Technology		Write down
16	Customer information security hacked ***Scenario: 3, 5***	Technology		Customer trust & write down
17	Whole network system failure due to human error ***Scenario: 2, 4, 5***	System		Loss or damage to asset
18	Whole network system failure due to defect network hardware ***Scenario: 2***	System		Loss or damage to asset
19	Whole network system failure due to software bug or virus ***Scenario: 2, 5***	System		Loss or damage to asset
20	Charging system failure ***Scenario: 1, 4, 5***	System		Write down
21	False transaction information between ATM –Tandem – Host ***Scenario: 1, 5***	System		Loss of recourse
22	Inefficient ATM system in used ***Scenario: 1, 2, 3, 4, 5***	Innovation		Loss of recourse
23	Lawsuits from unsatisfied customer	Legal	**External**	Legal liability
	Scenario: 1, 4, 5			
24	Vendor system cannot fulfill SLA (*Service Level Agreement*) ***Scenario: 2***	Legal		Loss of recourse
25	Negative publicity by unsatisfied customer ***Scenario:1,2,4, 5***	Reputation		Loss of recourse & restitution
26	Black campaign by certain irresponsible parties ***Scenario: 1,2,4, 5***	Reputation		Loss of recourse
27	Whole or particular network system down due to natural disaster ***Scenario: 2***	Natural Disaster	**Natural**	Loss or damage to asset

- *Stage-3:* ***Risk Assessment***

In calculating identified risks severity and likelihood, it will use qualitative and semi-quantitative method to calculate the severity and for determine the likelihood due to inadequate data of number which required for doing quantitative analysis. The following tables show the parameter to determine the value of probability and severity of the identified credit, operational and external risks.

TABLE III. Semi-Quantitative Risk Severity Parameter

Severity Level	**Quantitative**	**Qualitative**		
	Financial Implication (*X in Rp. mil*)	**Factor Influencing Shareholder Value**		
		Public Attention	Terms Violation	Customer Service
Insignificant (1)	X ≤ 50	Not attract any attention	Only internal administrative violation	Customer inconvenience can be ignored
Minor (2)	50 < X ≤ 150	Potential to attract attention	Internal terms violation which raises risk but not related to the transaction event	Customer inconvenience can be solved immediately
Moderate (3)	150 < X ≤ 250	Minor negative publicity by mass media	Internal terms violation which raises risk and related to the transaction event	Customer inconvenience takes 1 day to be solved

Major (4)	250 < X ≤ 500	Major negative publicity by mass media	Internal and external terms violation which raises risk related to the transaction event	Customer inconvenience takes more than 1 day to be solved
Significant (5)	X > 500	Lose the public's trust	Extreme Internal and external terms violation which raises risk related to the transaction event	All customer is not satisfied at all due to failure in solving the inconvenience

TABLE IV. Semi-Quantitative Risk Likelihood Parameter

Probability	Event Periods	Event Frequency per Year
Low (1)	> 1 year	≤ 1
Unlikely (2)	> 6 months & ≤ 1 year	2 – 3
Moderate (3)	> 3 months & ≤ 6 months	4 – 11
Likely (4)	> 1 month & ≤ 3 months	12 – 23
High (5)	≤ 1 month	≥ 24

For strategic or business risk, this project is using qualitative approach based on the management involvement in handling the risks and the level of risk event occurrences.

TABLE V. Qualitative Risk Severity Parameter

Risk Level	Management Involvement
Insignificant (1)	Acceptable without review by management
Minor (2)	Acceptable with review by management
Moderate (3)	Undesirable and requires corrective action, but some management discretion allowed
Major (4)	Undesirable and requires immediate corrective action
Significant (5)	Very undesirable and requires immediate change in the decision

TABLE VI. Qualitative Risk Likelihood Parameter

Probability	Event Occurences
Low (1)	Practically impossible
Unlikely (2)	Not likely to occur
Moderate (3)	Possibility of occurring sometimes
Likely (4)	Possibility of isolated incidents
High (5)	Possibility of repeated incidents

Using the parameter defined on the tables above, for each risk can be assigned severity and likelihood score to map the risk on the risk matrix based on Cox's theorem (2008) that can be seen on the table and figure below.

TABLE VII. Risk Score

No.	Event description	Severity	Likelihood	Total Risk
1	Poor acceptance of ATM services by customer	4	2	8
2	Competitor offer better ATM system for customer	2	1	2
3	Losing customers due to unsatisfied with the ATM services	4	2	8
Total Risk of Strategic Risk				**18**
4	Customer failed to pay his/her debt obligation	2	5	10
Total Risk of Credit Risk				**10**
5	Data center security violation	3	3	9
6	Fraud on payment server	3	1	3
7	Change of requirement on the current system	4	1	4
8	Limit budget on system maintenance	4	1	4
9	Data center not enough storage	2	2	4
10	Fail to follow-up and solve problems from customer complain	4	3	12
11	Data center overload due to poor load balance estimation	3	3	9
12	Particular network system failure due to human error	5	2	10
13	Particular network system failure due to defect network hardware	5	1	5
14	Particular network system failure due to software bug or virus	5	1	5
15	Fraud on ATM payment mechanism during regular downtime	4	1	4
16	Customer information security hacked	4	2	8
17	Whole network system failure due to human error	5	1	5
18	Whole network system failure due to defect network hardware	5	1	5
19	Whole network system failure due to software bug or virus	5	1	5
20	Charging system failure	2	2	4
21	False transaction information between ATM – Tandem – Host	1	5	5
22	Inefficient ATM	5	1	5

	system in used			
Total Risk of Operational Risk				**106**
23	Lawsuits from unsatisfied customer	2	1	2
24	Vendor system cannot fulfill SLA (*Service Level Agreement*)	4	1	4
25	Negative publicity by unsatisfied customer	5	3	15
26	Black campaign by certain irresponsible parties	5	3	15
27	Whole network system failure due to natural disaster	5	1	5
Total Risk of External Risk				**41**
Total of All Risks				**175**

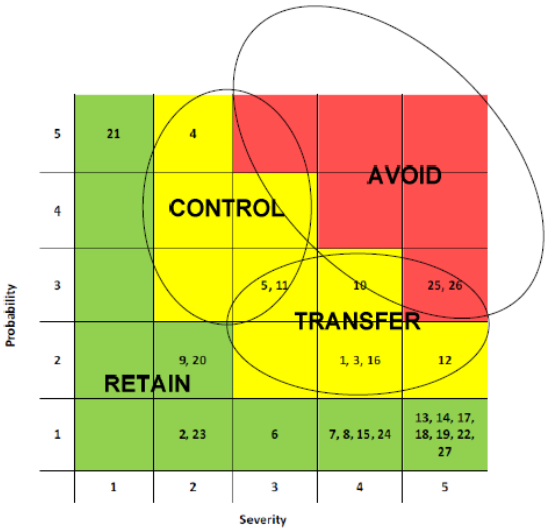

Figure 3. Risk Mapping on the Risk Matrix designed based on Cox's Theorem

- *Stage-4:* ***Risk Mitigation***

From the risk matrix on figure 5, appropriate mitigation plan need to be assigned based on the location of each risk. The following table listed all the appropriate risk mitigation for each risk.

TABLE VIII. Risk Mitigation

No.	Event description	Type of risk	Category of risk	Mitigation
1	Poor acceptance of ATM services by customer	Business	**Strategic**	Transfer
2	Competitor offer better ATM system for customer	Business		Retain
3	Losing customers due to unsatisfied with the ATM services	Business		Transfer
4	Customer failed to pay his/her debt obligation	Credit	**Credit**	Control
5	Data center security violation	People	**Operational**	Control
6	Fraud on payment server	People		Retain
7	Change of requirement on the current system	Process		Retain
8	Limit budget on system maintenance	Process		Retain
9	Data center not enough storage	Process		Retain
10	Fail to follow-up and solve problems from customer complain	Process		Transfer
11	Data center overload due to poor load balance estimation	Productivity		Control
12	Particular network system failure due to human error	Productivity		Transfer
13	Particular network system failure due to defect network hardware	Technology		Retain
14	Particular network system failure due to software bug or virus	Technology		Retain
15	Fraud on ATM payment mechanism during regular downtime	Technology		Retain
16	Customer information security hacked	Technology		Transfer
17	Whole network system failure due to human error	System		Retain
18	Whole network system failure due to defect network hardware	System		Retain
19	Whole network system failure due to software bug or virus	System		Retain
20	Charging system failure	System		Retain
21	False transaction information between ATM –Tandem – Host	System		Retain
22	Inefficient ATM system in used	Innovation		Retain
23	Lawsuits from unsatisfied	Legal	**External**	Retain

	customer			
24	Vendor system cannot fulfill SLA (*Service Level Agreement*)	Legal		Retain
25	Negative publicity by unsatisfied customer	Reputation		Avoid
26	Black campaign by certain irresponsible parties	Reputation		Avoid
27	Whole or particular network system down due to natural disaster	Natural		Retain

- *Stage-5:* ***Risk Report***

From the all the steps that have been done, the next step is building a risk report card consists of risk event, risk number, risk response action and its description as a reference for risk management group to discussed any further with the top management.

Risk Event	Poor acceptance of ATM services by customer
Risk Number	S-01
Risk Response Action	Transfer
Implementation	Create End User Agreement that defines the services acceptance by user when using the ATM services.

Risk Event	Losing customers due to unsatisfied with the ATM services
Risk Number	S-03
Risk Response Action	Transfer
Implementation	Create End User Agreement that defines the services acceptance by user when using the ATM services.

Risk Event	Customer failed to pay his/her debt obligation
Risk Number	CR-01
Risk Response Action	Control
Implementation	Analyze customer feedback about the problem and then reformulate with the responsible groups to design new system or update existing system.

Risk Event	Data center security violation
Risk Number	OP-01
Risk Response Action	Control
Implementation	Evaluate the weakness point and then reformulate with the responsible groups to design new system or update existing system.

Risk Event	Inefficient ATM system in used
Risk Number	OP-18
Risk Response Action	Retain
Implementation	Allocate some capital and ask system vendors to change or update the system seamlessly

Risk Event	Lawsuits from unsatisfied customer
Risk Number	E-01
Risk Response Action	Retain
Implementation	Allocate adequate capital for legal cost and restitution in case lost the trial.

.

Risk Event	Whole network system failure due to natural disaster
Risk Number	E-05
Risk Response Action	Retain
Implementation	Allocate some capital to cover the loss or the cost during system data recovery from DRC (Data Recovery Center)

IV. ANALYSIS & DISCUSSION

From the risk matrix figure, it shown that there are ten risks that can be categorized as high-priority risk:

- ✓ Risk event-1: Poor acceptance of ATM services by customer
- ✓ Risk event-3: Losing customers due to unsatisfied with ATM services
- ✓ Risk event-4: Customer failed to pay his/her debt obligation
- ✓ Risk event-5: Data center security violation
- ✓ Risk event-10: Fail to follow-up and solve problems from customer complain
- ✓ Risk event-11: Data center overload due to poor load balance estimation
- ✓ Risk event-12: Particular network system failure due to human error
- ✓ Risk event-16: Customer information security hacked
- ✓ Risk event-25: Negative publicity by unsatisfied customer
- ✓ Risk event-26: Black campaign by certain irresponsible parties

After identified all the high-priority risk on the possible scenarios, the next step is prioritizing which problem need to be solve by putting each risk to the problem based on the scenarios.

- **Problem-1**

  Daily critical down time – Full System Offline for maximum 12 minutes
  - o Poor acceptance of ATM services by customer
  - o Losing customers due to unsatisfied with ATM services
  - o Data center security violation
  - o Customer information security hacked
  - o Fail to follow-up and solve problems from customer complain
  - o Data center overload due to poor load balance estimation
  - o Particular network system failure due to human error
  - o Negative publicity by unsatisfied customer
  - o Black campaign by certain irresponsible parties
  - o Customer failed to pay his/her debt obligation
- **Problem-2**

  Tandem partition storage monitoring procedure

- Fail to follow-up and solve problems from customer complain
- Data center overload due to poor load balance estimation
- Losing customers due to unsatisfied with the ATM services
- Negative publicity by unsatisfied customer
- Black campaign by certain irresponsible parties
- Customer failed to pay his/her debt obligation

- **Problem-3**
  Tandem password security vulnerability
  - Data center security violation
  - Customer information security hacked
  - Negative publicity by unsatisfied customer
  - Black campaign by certain irresponsible parties
  - Particular network system failure due to human error
- **Problem-4**
  Base24 password security vulnerability
  - Data center security violation
  - Customer information security hacked
  - Negative publicity by unsatisfied customer
  - Black campaign by certain irresponsible parties
  - Particular network system failure due to human error
- **Problem-5**
  ATM technology specification and implementation used to be driven by vendors
  - Poor acceptance of ATM services by customer
  - Losing customers due to unsatisfied with ATM services
  - Data center security violation
  - Customer information security hacked
  - Fail to follow-up and solve problems from customer complain
  - Data center overload due to poor load balance estimation
  - Particular network system failure due to human error
  - Negative publicity by unsatisfied customer
  - Black campaign by certain irresponsible parties
  - Customer failed to pay his/her debt obligation

From the above list of high-priority risks on each problem, it can be concluded that **problem-1** and **problem-5** are categorized as a high-priority problem that need to be solve with an appropriate mitigation plan as it contain the all the high-priority risk.

V. CONCLUSION & RECOMMENDATION

As the result from the risk assessment done earlier, there are two problems with high-priority level that need to solve to improve the current ATM services. Those problems are

- ✓ Problem-1: **Daily critical down time – Full System Offline for maximum 12 minutes**

  This system process needs to be done to let data traffic handler switching from AS/400 to Tandem machine and vice versa, before and after AS/400 running its End-of-Day (EOD) batch job. During this period all ATM is unavailable and reject to do any transaction conduct by customer. This switching process is started manually by the operator (in this case Bank XYZ's IT operation staff) not long before 11:59 PM and will started again after EOD batch job done, usually it finish before 06:00 AM on the next morning.
- ✓ Problem-2: **ATM technology specification and implementation used to be driven by vendors**

ATM technology specification and implementation is used to be driven by vendors without considering the specifications those are really needed to provide customers with excellence services. This research offered a solution for both problems by encouraging Bank XYZ's to design its own ATM system with the specification that can fulfill their need in order to improve the ATM services. The proposed system improvement is called "Offline Transaction ATM System" that been designed to solve the first problem with minimum change on whole current ATM system.

Offline Transaction ATM System

Definition	:	ATM system which can still run during critical down time (host is offline) to support 24 x 7 hours ATM services
System Limitation	:	– Any transaction that involve other customer account is not available (open transfer) – Any transaction that are using interbank ATM network such as ATM Link/ATM Bersama is not available
Specific ATM specification	:	– Card reader + writer – Card with data capacity over 4 KB (kilobyte) – HSM – Software application to control the offline system (in Host and ATM)
Information and data keep on the ATM storage	:	– Card number – PIN (encrypted) – Type of transaction – Balance information before and after transaction

Offline transaction ATM system is active after host system sent going offline (system down) notification to the tandem machine. The tandem machine notifies ATM machines to activate Offline transaction ATM system procedure before the host is offline. When the procedure has been activated and host is offline, ATM start to check the customer whose doing transaction during critical down time by doing verification of customer data directly from the customer card. At this point ATM system also doing card data validation to make sure the card has not been tampered before (or the data has been manipulated). In PIN validation process, ATM is

verifying PIN input by customer by reading PIN data from the customer card. If it is valid, ATM will send the PIN to HSM for further verification. All the transaction done by the customer is being record to the temporary local storage in ATM.

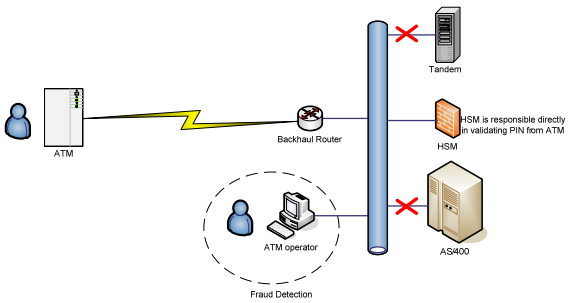

Figure 4. Offline Transaction ATM System Topology

After the host system is going back online, host system sends notification to the tandem machine that it is going back online. Tandem machine sends the notification to ATM machines to deactivate offline procedure and prepare to go online and doing database synchronization with the host. Host system verifies all the transaction during offline by comparing customer balance information before doing transaction with the last balance data on the host database. If it is valid or no suspicious problem, host will update the data on the database with the new data. If it is invalid, host system will notify ATM operator to investigate the problem about the potential of fraud done by the customer. In order this system is successfully implemented, Bank XYZ's has to push the technology vendors to follow this system design and always check the fact whether if it is true or not when the technology vendors tell if there is something in this design is impossible to fulfill. In order to successfully to do this, Bank Mandiri's has to improve its ***Policy*** and ***Standard Operating Procedure*** (SOP) in project tendering to prevent certain people inside doing inappropriate action for personal benefits during the project with the vendors. Bank Mandiri does also need to provide risk management training to improve employees risk awareness about the inherent risk derived from the new system.

Conclusion

By having the obligation to provide high quality services, Bank XYZ as a well-known public banking service institution need to always improve its products and services to accommodate the most recent customer needs. By improving its ATM system in order to increase its ATM quality of services, Bank XYZ can prove that it can give its customers excellence services and good user experience while doing transaction at ATM.

This research shows that by implement risk-based audit with customer focus method, the firm could fulfill its tag-line or promise to give "*24x7 hours excellence ATM services*". Moreover, through the implementation of proposed new ATM system, Bank XYZ could explore new opportunity to attract numbers of new customer and achieve its objectives. Hopefully, by implementing the result of this research, Bank XYZ could increase its ATM service quality and ensure its service delivery sustainability to the society.

ACKNOWLEDGMENT

This paper is written based on the author's final project at MBA - ITB supervised by Prof.Dr.Ir.Sudarso Kaderi Wiryono who has been relentlessly motivating the author to accomplish the final project. The author would like to thank you Company XYZ where the final project has taken place.

REFERENCES

Audittindo Education, 2006, *An Introductory Course for Implementing Risk-Based Auditing,* PT Audittindo Arin Prima, Jakarta.

Arens, Alvin A, Randal J. Elder, Mark S. Beasley, 2003, *Auditing dan Pelayanan Verifikasi: Pendekatan Terpadu*, PT Indeks, Jakarta.

Bank Indonesia, 2001, Peraturan Bank Indonesia *No 3/23/PBI/2001, tentang Penerapan Prinsip Mengenal Nasabah (Know Your Customer Principles)*, Bank Indonesia, Jakarta.

Bank Indonesia, 2003, Peraturan Bank Indonesia *No 5/8/PBI/2003, tentang Penerapan Manajemen Risiko Bagi Bank*, Bank Indonesia, Jakarta.

Bank Indonesia, 2004, Peraturan Bank Indonesia *No 6/30/PBI/2004, tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu*, Bank Indonesia, Jakarta.

Bank Indonesia, 2003, Surat Edaran Bank Indonesia no.5/22/DPNP, perihal *Pedoman Standar Sistem Pengendalian Intern bagi Bank Umum,* Bank Indonesia, Jakarta.

Bank Indonesia, 2004, Surat Edaran Bank Indonesia no.6/18/DPNP, perihal *Penerapan Manajemen Risiko Pada Aktivitas Pelayanan Jasa Bank Melalui Internet*, Bank Indonesia, Jakarta.

Bank Indonesia, 2004, Surat Edaran Bank Indonesia no.6/37/DPNP, perihal *Penilaian dan Pengenaan Sanksi atas Penerapan Prinsip Mengenal Nasabah dan Kewajiban Lain Terkait Dengan Undang-Undang tentang Tindak Pidana Pencucian Uang*, Bank Indonesia, Jakarta.

Bank Indonesia, 2004, Surat Edaran Bank Indonesia no.7/60/DASP, perihal *Prinsip Perlindungan Nasabah dan Kehati-hatian, serta Peningkatan Keamanan Dalam Penyelenggaraan Kegiatan Alat Pembayaran dengan Menggunakan Kartu*, Bank Indonesia, Jakarta.

Bank XYZ, 2011, *Bank XYZ: Technology and Operations*, Bank XYZ, Jakarta.

Bank XYZ, 2011, *Bank XYZ: Risk Management*, Bank XYZ, Jakarta.

Bank XYZ, 2011, *IT Risk Management Plan (IT-RMP)*, Bank XYZ, Jakarta.

Bank XYZ, 2012. *Corporate Profile & Transformation Process*. Bank XYZ, Jakarta.

Bank XYZ, 2012. *Financial Fundamentals*. Bank XYZ, Jakarta.

Bank XYZ, 2012. *GCG Charter*. Bank XYZ, Jakarta.

Bank XYZ, 2012. *Management Team*. Bank XYZ, Jakarta.

Basel Committee on Banking Supervision, 1997, *Core Principles for Effective Banking Supervision*.

Cox, L. A. Jr., 2008, *What's Wrong with Risk Matrices?*, Risk Analysis, Vol. 28 No. 2

Davis, G.B. 1992. *Kerangka Dasar Sistem Informasi Manajemen: Struktur dan Perkembangannya*. PT Pustaka Binaman Pressindo, Jakarta.

Hewlett Packard. 2006. *Guardian User's Guide.* Jakarta.

INTOSAI, 2008. *Information Technology Audit General Principles*. Office of The Comptroller and Auditor General, India.

Namee, David Mc, et all, 1998, *Risk Management: Changing The Internal Auditor's Paradigm*, Institute Of Internal Auditors Research Foundation, Altamore, Sping, Florida.

NCR. 2001. *PersonaS77ATM Operator Manual.* NCR Corp: Ohio, USA.

O'Brien, J.A. 2006. *Pengantar Sistem Informasi: Perspektif Bisnis dan Manajerial*. Penerbit Salemba Empat, Jakarta.

Robert Tampubolon, 2005, *Risk and Systems-Based Internal Auditing*, PT Elex Media Komputindo, Jakarta

Rot, Artur, 2008, *IT Risk Assessment: Quantitative and Qualitative Approach*, WCECS Oct.24 – 28, 2008, San Fransisco, USA

The Institute of Internal Auditors, 1991, *Statement on Internal Auditing Standards (SIAS) no.9: Risk Assessment,*. 249 Maitland Avenue, Altamonte Springs, Florida.

Woodbury, Carol. 2000. *Implementing AS/400 Security: 4th Edition*. News/400 Books. Colorado.